Privacy Act 101

Orientation training for all Military Members, Civilian Employees, and Contractor Personnel

What is the Privacy Act?

The Privacy Act is an Act to limit an Agency's collection and sharing of personal data. The Privacy Act requires that all Executive Branch Agencies follow certain procedures when:

Collecting personal information

Creating databases containing personal identifiers

Maintaining databases containing personal identifie

Disseminating information containing personal data

Why was the Privacy Act passed?

Roots of the Privacy Act of 1974 can be traced as far back as 1965 when hearings were held by the House of Representatives Special Subcommittee on Invasion of Privacy. The Privacy Act was created in response to concerns about how the creation and use of computerized databases might impact individuals' privacy rights. It safeguards privacy through creating four procedural and substantive rights in one's own personal data.

1.
It requires government agencies to show an individual records that are kept on that individual.

2.
It requires agencies to follow certain principles, called "fair information practices," when gathering and handling personal data.

3.
It places restrictions on how agencies can share an individual's data with other people and agencies

4.
It lets individuals sue the government for violating the provisions of the Act.

Why was the Privacy Act enacted?

The Privacy Act was passed to address past abuses such as:

- **Federal strong-arm tactics for data collection**
- **Federal misuse of personal data**
- **Growing impact of computer technologies and the potential for abuse**

With the abuses that took place during Watergate, and the growing use of computers to store information, Congress envisioned the damage that could occur to personal privacy in a computer-based society.
This realization lead to the creation of the Privacy Act.

What are the limitations of the Privacy Act?

The Privacy Act applies only to:

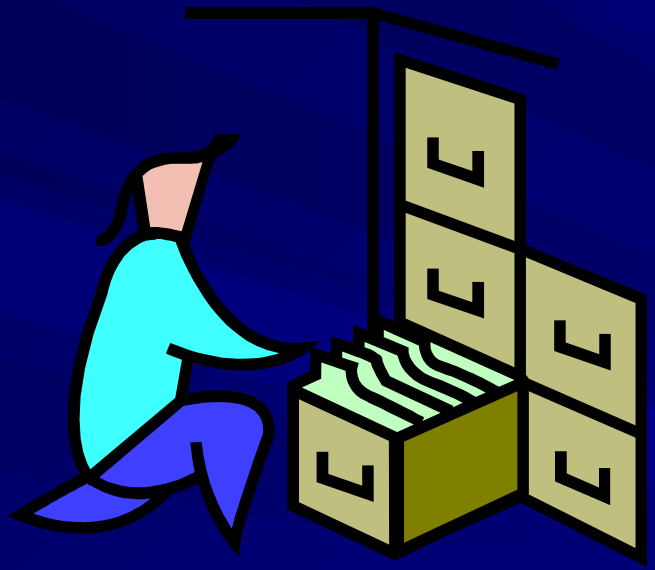
US citizens

or

Lawfully admitted aliens

Whose records are filed in a "System of Records" where those records are retrieved by a personal identifier.

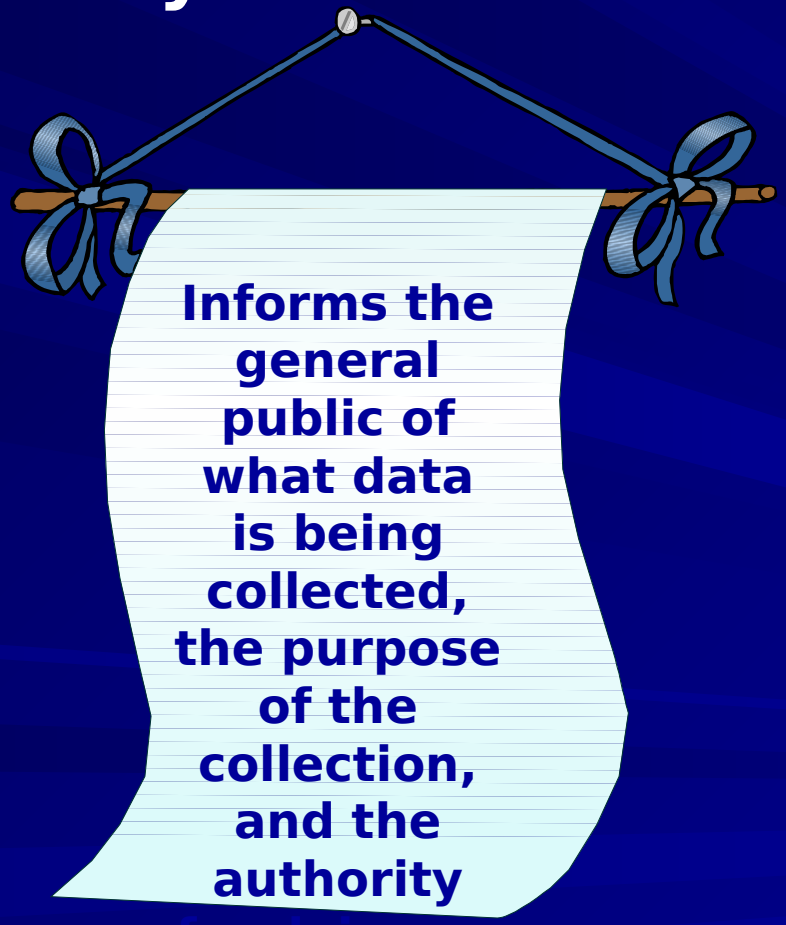
What is a System of Records?

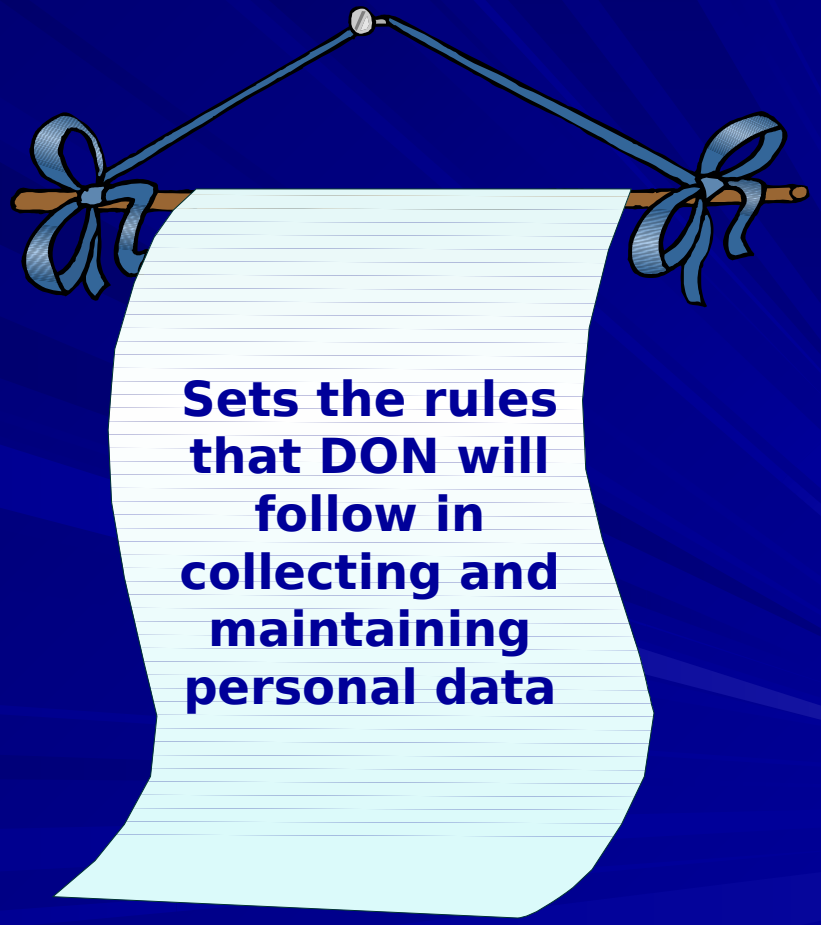


- **A System of Records is a group of records that:**
  - **Contains a personal identifier (such as a name, Social Security Number, Employee Number, etc.)**
  - **Contains one other item of personal data (such as home address, performance rating, blood type, etc.)**
  - **Is retrieved by a personal identifier.**

What purpose does the System Notice serve?

- **A System Notice:**





What specific data is listed in a System Notice?

- **A System Notice includes:**

System Location: Tells where files are located

Categories of individuals covered by the system: Tells what people are covered

Categories of records in the system: Tells what data elements are collected

Authority of maintenance of the system: Gives legal authority to collect and maintain the information in the system

Purpose(s): Tells how DON will use the information internally

Routine uses of records maintained in the system, including categories of users and purposes of such uses

Lists agencies outside of DOD that will have access to the information and how they are authorized to use

What specific data is listed in a System Notice? (cont'd)

A System Notice also includes the following:

Policies and practices for storing, retrieving, accessing, retaining, and disposing of records contained in the system

Storage: States whether files are in paper or electronic form

Retrievability: Lists the information that is needed to retrieve a file (such as SSN)

Safeguards: Describes the protections established to safeguard the records

Retention and Disposal: Tells how long the records are kept before are destroyed

System manager(s) and address: Gives us the physical address of t manager of record for the system

Notification Procedures: Tells how you can learn if you are in the sy

What specific data is listed in a System Notice? (cont'd)

A System Notice also includes these categories of data:

Record Access Procedures: Tells what steps you mu
to see your own record

Contesting Record Procedures: Tells what steps you
take to correct errors in your file

Record Source Categories: Tells who provided the information to DON

Exemptions Claimed for the System: States whethe
has claimed a Privacy Act exemption for this s

What are DON's responsibilities under the Privacy Act?

DON must:

- **Establish rules of conduct for collecting, maintaining, and dis**
  Protected Personal Information (PPI)
- **Publish Privacy Act System Notices in the Federal Register**
- **Collect only data that is authorized by law**
- **Share data with authorized recipients only**
- **Establish and apply data safeguards**
- **Allow individuals to review records about themselves**
- **Allow individuals to amend their personal records containing**
- **Keep a record of disclosures made to authorized recipients**

What are DON's responsibilities under the Privacy Act? (cont'd)

DON must:

Provide the record subject, upon request, with a list of all authorized d upon request made

With some exceptions, make no disclosure without the record subject's written consent

Maintain only accurate, complete, timely, and relevant data

Provide a Privacy Act statement advising of the authority for the collec data and how it is to be used when collecting data on forms or surveys websites

In addition to the above, when contracts are awarded that involve Privacy Act data, DON must ensure that the contract contains the appropriate Federal Acquisition Regulation (FAR) privacy clauses.

What are my responsibilities as a DON employee?

- **As an employee, you play a very important role in assuring that DON complies with the provisions of the Privacy Act.**

- **Do not collect personal data without proper authorizat**
- **Do not distribute or release personal information to ot employees unless you are convinced that the release i**
- **Don’t be afraid to challenge ANYONE who asks to see P Act information for which you are responsible.**
- **Do not maintain records longer than permitted to do s**
- **Do not destroy records before disposal requirements a**
- **Do not place unauthorized documents in records syste**

What are my responsibilities as a DON employee? (Cont'd)

- **Do not commingle information about different individua in the same file.**

  Mark privacy records appropriately.
  "For Official Use Only – Privacy Act Sensitive"

- **Do not use interoffice or translucent envelopes to mail Act protected data. Instead, use sealable opaque solid Kraft envelopes. Be sure to mark the envelope to the p attention.**

- **Do not place PPI on shared drives, multi-access calenda the Intranet, or the Internet.**

- **Do not create "Systems of Records" on your computer, in your files without first contacting your Privacy officia**

I am a contractor. Does the Privacy Act apply to me?

Yes. Government contractors are subject to the Privacy Act and must comply with all of its provisions.

What are the penalties for violating the Privacy Act?

For knowingly and willfully requesting or obtaining records under false pretenses:

Misdemeanor criminal charge, and a fine of up to $5000.00

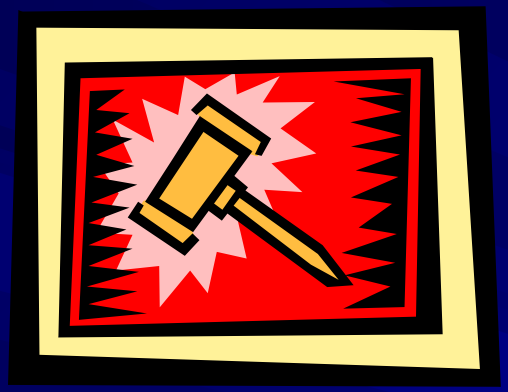
For knowingly and willfully disclosing privacy data to any person not entitled to access:

Misdemeanor criminal charge, and a fine of up to $5000.00

For maintaining a System of Records without meeting the public notice requirements:

Misdemeanor criminal charge, and a fine of up to $5000.00

What are the penalties for violating the Privacy Act? (cont'd)



- **Courts may award civil penalties for the following:**
  - **Unlawfully refusing to amend a record**
  - **Unlawfully refusing to grant access to a record**
  - **Failure to maintain accurate, relevant, timely, and complete data.**
  - **Failure to comply with any Privacy Act provision OR agency rule that results in an adverse effect on the subject of the record.**

Penalties for these violations include:
Actual Damages
Payment of reasonable attorney's fees
Removal from employment

How will I know if the data that I handle is Privacy Act protected data?

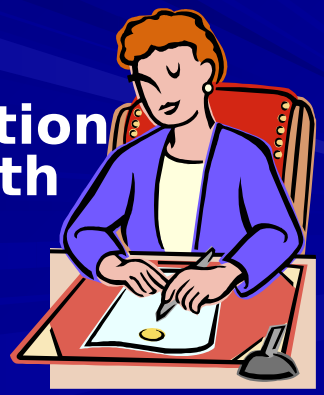
- **PPI should be marked: "For Official Use Only – Privacy Sensitive: Any misuse or unauthorized disclosure may result in both civil and criminal penalties."**
- **Be aware that PPI may not always be marked as such. If you have questions about whether data is protected under the Privacy Act, ask your supervisor.**

What is the DON Code of Fair Information Principles?

- **In order to assure that any personal information submitted to DON is properly protected, DON has devised a list of principles to be applied when handling personal information. This is referred to as the "Code of Fair Information Principles"**

- **The "Code of Fair Information Principles" is set forth in a list of 10 policies that DON employees will follow when handling personal information.**

- **Any DON employee, military member, or contractor who handles the personal information of others must abide by the principles set forth by the Code.**



The DON Code of Fair Information Principles

1. <u>The Principle of Openness</u>: When we collect personal data from we will inform you of the intended uses of the data, the disclosures will be made, the authorities for the collection, and whether the co is mandatory or voluntary. We will collect no data subject to the Pr unless a Privacy Act system notice has been published in the Feder Register and posted on the and at www.privacy.navy.mil.

2. <u>The Principle of Individual Participation</u>: Unless DON has claime exemption from the Privacy Act, we will, upon request, grant you a your records; provide you a list of disclosures made outside the De of Defense ; and make corrections to your file, once shown to be in

3. <u>The Principle of Limited Collection</u>: DON will collect only those data elements required to fulfill an official function or mission grou law. Those collections are conducted by lawful and fair means.

Besides Privacy Act data, should I be concerned with other types of For Official Use Only (FOUO) data?

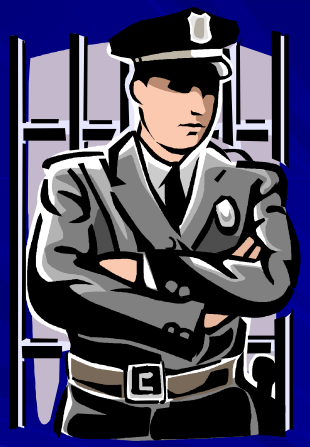
Yes! **As an employee, you will come in contact with multiple types of records. Some may be marked as "FOUO." For data marked as FOUO, you must:**

Properly safeguard it.

Use it only for official government busine

Share it only with those with an official n for access.

If you create records containing FOUO da mark them at the time of creation.



Not all records are marked with the FOUO legend. If the record is not marked as FOUO, you may still be required to safeguard it.

Do not disclose any agency record to a third party except for official, authorized purposes.

What are some examples of FOUO data?

- **Data that could allow someone to circumvent DLA rules or commit fraud.**
  - **Examples:**
    - **Government credit card account numbers**
    - **Security plans, procedures, weaknesses and vulnerabilities**
    - **Answers to test questions**
    - **Guidelines for detecting fraud**
    - **Benchmarks and criteria used in evaluating job applicants**
    - **Procedures for securing assets, firearms, and controlled forms and devices**
    - **Procedures for identifying, neutralizing, or responding to security threats**
- **Data required by law to be handled as FOUO.**
  - **Examples:**
    - **Unsuccessful contractor proposals**
    - **Financial Disclosure Reports of special government employees**
    - **Dispute resolution communications**
    - **Drug abuse rehabilitation records**
    - **Names, duty addresses (including e-mail), and phone numbers of overseas employees.**

What are some examples of FOUO data? (cont'd)

- **Data submitted by private entities with th understanding it would be kept in confide**
  - **Examples:**
    - **Names of a company's customers, suppliers, and subcontractors**
    - **Business, financial, pricing, and management strategies**
    - **Profit and loss data, break-even calculations**
    - **Technical, cost, and management proposals**
    - **Assets, liabilities and net worth**
    - **Selling prices, purchase records, actual cost data**
    - **Unannounced future or planned products**
    - **Descriptions of plants or facilities, assembly line setups**
    - **Internal security measures**
    - **Scientific and manufacturing processes**

What are some examples of FOUO data? (cont'd)

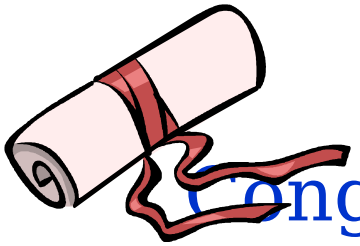
- **Government Privileged data.**
  - **Examples:**
    - **Internal advice, opinions, and recommendations.**
    - **Non factual portions of evaluations of contractors and their products.**
    - **Drafts or proposed policies, statements, reports, etc.**
    - **Confidential communications between attorney and client.**
    - **Documents prepared by an attorney in anticipation of actual or potential litigation.**
    - **Government background documents used to calculate its bid in a "contracting out" procedure (i.e., OMB Circular A-76).**
    - **Formulas or methods for evaluating contractor proposals.**

- **Investigative records**
  - **Examples:**
    - **Details that could compromise ongoing investigations**
    - **Investigative sources, techniques, and methods**
    - **Personal details about witnesses and third parties**

What are some examples of FOUO data? (cont'd)

- **Personal data about individuals.**
  - **Examples:**
    - **Financial, credit, and medical data.**
    - **Security clearance level.**
    - **Leave balances; types of leave used.**
    - **Home address and telephone numbers (including home web addresses).**
    - **Social Security Number.**
    - **Mother's maiden name; other names used.**
    - **Drug test results and the fact of participation in rehabilitation programs.**
    - **Family data.**
    - **Religion, race, national origin.**
    - **Performance ratings.**
    - **Names of employees who hold government-issued travel cards, including card data**

Certificate of Completion



Congratulations on the completion of

Privacy Act 101

Orientation training for all

Military Members, Civilian Employees, and Contractors